

CLAIMS

What is claimed is:

1. Apparatus for ensuring the integrity of computer applications to be run in association with a computer having data storage arranged sectorwise in a storage device, comprising
an identifier for identifying an application to be run,
a listing associated with at least one of said applications to be run, said listing identifying different sectors of said storage device and associating with each identified sector an access level required by said application, and
an enforcement device, for prohibiting said at least one application from accessing an identified sector of said storage device at any level higher than said associated required access level.
2. Apparatus for ensuring the integrity of computer applications to be run in association with a computer having data storage arranged sectorwise in a storage device, comprising
an identifier for identifying an application to be run,
a listing associated with at least one of said applications to be run, said listing identifying different sectors of said storage device and associating with each identified sector an access level,
an enforcement device, for preventing said at least one application from accessing an identified sector of said storage device at any level higher than said associated access level, and
a query device, for identifying when an attempt to access a sector of said storage device has been prevented by said enforcement device, querying said attempt with said user, and if found acceptable then including said higher level of access in said listing.
3. Apparatus for ensuring the integrity of computer applications to be run in association with a computer having data storage arranged sectorwise in a storage device, comprising
an identifier for identifying an application to be run,

a listing associated with at least one of said applications to be run, said listing identifying different sectors of said storage device and associating with each identified sector an access level, an enforcement device, for preventing said at least one application from accessing an identified sector of said storage device at any level higher than said associated access level, and a query device, for identifying when an attempt to access a sector of said storage device has been prevented by said enforcement device, querying said attempt against a predetermined configuration, and if found acceptable then including said higher level of access in said listing.

4. Apparatus according to claim 2 wherein said query device continues to query such attempts for the duration of one of a predetermined time period and a predetermined number of access attempts.

5. Apparatus according to claim 3 wherein said query device continues to query such attempts for the duration of one of a predetermined time period and a predetermined number of access attempts.

6. 0 *Final Note* Apparatus according to claim 2 wherein said query device continues to query such attempts until the next occasion upon which said computer is reset.

7. Apparatus according to claim 3 wherein said query device continues to query such attempts until the next occasion upon which said computer is reset.

8. Apparatus for ensuring the integrity of computer applications to be run in association with a computer having data storage arranged sectorwise in a storage device, comprising an identifier for identifying at least one application to be run,

00937883-002597

said at least one application being adapted to call at least one other application to run,
a listing associated with at least one of said applications to be run, said listing identifying
different sectors of said storage device and associating with each identified sector an access level
required by said application,

an enforcement device, for prohibiting said at least one application from accessing an
identified sector of said storage device at any level higher than said associated required access level,
and

wherein said identifier is adapted firstly to identify a listing associated with said at least
one other application for use with said enforcement device, and if such a listing cannot be found then
identifying a listing associated with said at least one application for use with said enforcement device.

9. A computer connected to a network, said computer comprising a storage device for
storing data, a transmission device for sending data from said computer to said network, a listing of
controlled data which should not be sent to said network, a comparison device adapted to compare
data sent to said transmission device with said controlled data, and a prevention device for
preventing data corresponding to said controlled data being sent automatically to said network.

10. Apparatus according to claim 1 further comprising override means adapted to allow an
operator to override said enforcement means.

11. Apparatus according to claim 8 further comprising override means adapted to allow an
operator to override said enforcement means.

12. Apparatus according to claim 9 further comprising override means adapted to allow an
operator to override said prevention means.

00927883 092597
465260 "E887E680

13. Apparatus for ensuring the integrity of computer applications to be run in association with a computer having data storage arranged sectorwise in a storage device, comprising
an identifier for identifying at least one application to be run,
said at least one application being adapted to call at least one other application to run,
a listing associated with at least one of said applications to be run, said listing identifying different sectors of said storage device and associating with each identified sector an access level required by said application,

an enforcement device, for prohibiting said at least one application from accessing an identified sector of said storage device at any level higher than said associated required access level,
and

a query device, for identifying when an attempt to access a sector of said storage device has been prevented by said enforcement device, querying said attempt with a user, and if found acceptable then including said higher level of access in said listing,

wherein said identifier is adapted firstly to identify a listing associated with said at least one other application for use with said enforcement device, and if such a listing cannot be found then identifying a listing associated with said at least one application for use with said enforcement device.

14. Apparatus for ensuring the integrity of computer applications to be run in association with a computer having data storage arranged sectorwise in a storage device, comprising
an identifier for identifying at least one application to be run,
said at least one application being adapted to call at least one other application to run,
a listing associated with at least one of said applications to be run, said listing identifying different sectors of said storage device and associating with each identified sector an access level required by said application,

an enforcement device, for prohibiting said at least one application from accessing an identified sector of said storage device at any level higher than said associated required access level, and

a query device, for identifying when an attempt to access a sector of said storage device has been prevented by said enforcement device, querying said attempt against a predetermined configuration, , and if found acceptable then including said higher level of access in said listing,

wherein said identifier is adapted firstly to identify a listing associated with said at least one other application for use with said enforcement device, and if such a listing cannot be found then identifying a listing associated with said at least one application for use with said enforcement device.

15. A computer connected to a network, said computer comprising a storage device for storing data sectorwise, a transmission device for sending data from said computer to said network, a listing of controlled data which should not be sent to said network, a comparison device adapted to compare data sent to said transmission device with said controlled data, and a prevention device for preventing data corresponding to said controlled data being sent automatically to said network, said computer further comprising

an identifier for identifying an application to be run,

a listing associated with at least one of said applications to be run, said listing identifying different sectors of said storage device and associating with each identified sector an access level required by said application, and

an enforcement device, for prohibiting said at least one application from accessing an identified sector of said storage device at any level higher than said associated required access level.

16. A computer connected to a network, said computer comprising a storage device for storing data sectorwise, a transmission device for sending data from said computer to said network, a listing of controlled data which should not be sent to said network, a comparison device adapted to compare data sent to said transmission device with said controlled data, and a prevention device for

preventing data corresponding to said controlled data being sent automatically to said network, said computer further comprising

an identifier for identifying an application to be run,

a listing associated with at least one of said applications to be run, said listing identifying different sectors of said storage device and associating with each identified sector an access level,

an enforcement device, for preventing said at least one application from accessing an identified sector of said storage device at any level higher than said associated access level, and

a query device, for identifying when an attempt to access a sector of said storage device has been prevented by said enforcement device, querying said attempt with a user, and if found acceptable then including said higher level of access in said listing.

17. A computer connected to a network, said computer comprising a storage device for storing data sectorwise, a transmission device for sending data from said computer to said network, a listing of controlled data which should not be sent to said network, a comparison device adapted to compare data sent to said transmission device with said controlled data, and a prevention device for preventing data corresponding to said controlled data being sent automatically to said network, said computer further comprising an identifier for identifying at least one application to be run,

said at least one application being adapted to call at least one other application to run,

a listing associated with at least one of said applications to be run, said listing identifying different sectors of said storage device and associating with each identified sector an access level required by said application,

an enforcement device, for prohibiting said at least one application from accessing an identified sector of said storage device at any level higher than said associated required access level, and wherein said identifier is adapted firstly to identify a listing associated with said at least one other application for use with said enforcement device, and if such a listing cannot be found then identifying a listing associated with said at least one application for use with said enforcement device.

08937883 092597

18. A computer connected to a network, said computer comprising a storage device for storing data sectorwise, a transmission device for sending data from said computer to said network, a listing of controlled data which should not be sent to said network, a comparison device adapted to compare data sent to said transmission device with said controlled data, and a prevention device for preventing data corresponding to said controlled data being sent automatically to said network, said computer further comprising

an identifier for identifying at least one application to be run,

said at least one application being adapted to call at least one other application to run,

a listing associated with at least one of said applications to be run, said listing identifying different sectors of said storage device and associating with each identified sector an access level required by said application,

an enforcement device, for prohibiting said at least one application from accessing an identified sector of said storage device at any level higher than said associated required access level, and

a query device, for identifying when an attempt to access a sector of said storage device has been prevented by said enforcement device, querying said attempt against a predetermined configuration, and if found acceptable then including said higher level of access in said listing,

wherein said identifier is adapted firstly to identify a listing associated with said at least one other application for use with said enforcement device, and if such a listing cannot be found then identifying a listing associated with said at least one application for use with said enforcement device.

Added
A1